And the Human Saves the Day or Maybe They Ruin It, The Importance of Humans in the Loop

Diana L. DeMott [1]
Science Applications International Corporation (SAIC), Houston, Texas, 77058

and

Roger L. Boyer[2]
National Aeronautics and Space Administration (NASA), Houston, Texas, 77058

Flying a mission in space requires a massive commitment of resources, and without the talent and commitment of the people involved in this effort we would never leave the atmosphere of Earth as safely as we have. When we use the phrase "humans in the loop", it could apply to almost any endeavor since everything starts with humans developing a concept, completing the design process, building or implementing a product and using the product to achieve a goal or purpose. Narrowing the focus to spaceflight, there are a variety of individuals involved throughout the preparations for flight and the flight itself. All of the humans involved add value and support for program success. The paper discusses the concepts of human involvement in technological programs, how a Probabilistic Risk Assessment (PRA) accounts for the human in the loop for potential missions using a technique called Human Reliability Analysis (HRA) and the tradeoffs between having a human in the loop or not. Human actions can increase or decrease the overall risk via initiating events or mitigating them, thus removing the human from the loop doesn't always lowers the risk.

I. Introduction

There's no denying that humans can perform extraordinary feats of brilliance to "save the day" as well as epic failures creating or adding to troubles that "ruin the day". Decisions made under extreme circumstance would be described as correct if the outcome is favorable, but those same decisions and actions could also be described as "human error" if the result is a tragic failure. The difference between a good decision or action and a bad one is often identified by the result, and when dealing with interactions of complex processes and systems there are multiple ways to produce an acceptable result or failure. Given the number of variables at play in these types of situations, it is often difficult to know the outcome in advance. It is much easier to look at the situation in hindsight and pronounce its cause as human error. In reality, humans are always involved somewhere. Even automated systems are designed, built, programmed, tested, maintained and operated by humans.

A PRA model is used to organize information for the various obstacles to mission success and identify potential risk contributors. These risks can be defined as threats to the project's ability to meet objectives including: safety, loss of life, human injury, environmental damage, operational capability, performance, technical and design requirements, cost, or schedule. PRA's are generally used for complex systems with high risk consequences with the intent of avoiding these outcomes.

An effective PRA looks at system and process interactions and can identify where apparently minor failures can affect the system as a whole. Using the definition of risk as a feasible unfavorable outcome, identification of risk can be answered by three questions: (1) what can go wrong, (2) what is the likelihood of the potential events or scenarios and (3) what consequences could result from these events or scenarios?

PRA and HRA were introduced into the NASA culture after the Space Shuttle had been flying for a number of years and experienced a major accident. The intent behind any risk assessment program is to identify potential risks associated with the identified goal (e.g. missions in the case of spaceflights) and analyze the concerns and consequences surrounding potential failure. Identifying and quantifying potential risks offers management an additional tool in the decision making process regarding whether to eliminate, mitigate or accept the consequences of the identified risks[1]. Direct human actions are covered by the human reliability assessments, while software

[1] Sr. HRA/PRA Analyst, Analysis Section.
[2] Risk and Reliability Analysis Branch Chief, Safety & Mission Assurance Directorate, Johnson Space Center.

reliability values include potential human errors in development and testing, and equipment/system reliability values also include human errors in development and installation actions.

II. Human Action Risk Contributions

HRA as defined in a PRA model captures the risk associated with direct interactions between humans and equipment (aka, man-machine interface, human systems interaction, etc.), and predicts the impact of these interactions on the probability of overall mission failure. NASA personnel are highly trained and qualified, however, even the most highly qualified and trained individuals are susceptible to making errors that could impact the mission or crew. Therefore, human reliability is included in PRA models. Human reliability represents the potential for humans to make a mistake given the variables inherent in a situation. The HRA is an evaluation of how an individual could act given the parameters of a defined failure scenario. It is not intended to place blame.

Not all human errors have serious consequences. In the majority of cases they are unimportant, annoying or self-corrected. Often, the way humans react to changing conditions are the only reason a process will continue to work. Unfortunately this flexibility in human actions can also cause what we describe as human errors. "The ability to adapt and compensate comes at a cost"[2]. The Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications[3] identifies some of these types of errors as:

- Errors of omission and commission
- Slips/lapses, mistakes, and circumventions
- Skill-, rule-, and knowledge-based errors
- Information processing errors including items such as detection and situation assessment

When human errors are viewed as a single risk driver, questions have arisen concerning the value of humans operating as part of the system. Attempting to remove the human from the equation and changing potential human error failure scenarios into automated actions could have consequences. When considering future manned spaceflight missions these consequences could include:

1) When using software settings to determine when to abort there are questions regarding what to use as trigger points when conditions can vary, and how to avoid unnecessary Loss of Mission (LOM) because the automated system is too rigid.
2) Automating activation of abort functions based on specific parameters defined with limited information may be based on conservative assumptions and create unnecessary LOM,
3) Some potential vehicle separation issues may need crew intervention.
4) Even with software controlled unmanned missions humans are involved with developing software codes, and uploading code and instructions to the spacecraft.
5) Loss of flexibility and capability for the overall system since humans can backup multiple systems, perform multiple functions and fit individual incidents into the "big picture".
6) Automated systems cannot address potential situations that have not been identified but could escalate into failure events.

Relying on software for expected or routine events may improve the reliability as long as all functions are identified and operate as expected. However, space flights are rarely routine and unexpected situations and unanticipated failures that affect software performance may occur and cause a LOM or Loss of Crew (LOC). This is especially true for new launch vehicle designs, exploration missions and activities intended to expand human knowledge. Using only automated systems would eliminate the opportunity for crew members to positively affect the event outcome.

Table 2-1 provides a comparison of the risks involved with crew members in the loop and when crews are excluded and cannot interact with the flight system.

Table 2-1: Automated Flight Controls with Humans as Backup

Inherent risks involved with using humans in the loop	Inherent risks of not using humans in the loop
Cause a failure (errors of omission and commission)	Lose flexible backup
Not react in time (slips/lapses, mistakes, and	Lose limited maintenance capability for minor repairs

circumventions)	
Misinterpret or misunderstand (skill-, rule-, and knowledge-based errors or information processing errors including items such as detection and situation assessment)	Lose oversight and minor problems dealt with as they arise
Right action, wrong time (skill-, rule-, and knowledge-based errors or information processing errors including items such as detection and situation assessment)	Failure is failure, software doesn't adapt unless in the programming
Bad decisions cause failures (skill-, rule-, and knowledge-based errors or information processing errors including items such as detection and situation assessment)	Does not react to any visual or physical "cues" not in the programing
Bad decisions contribute to failure (skill-, rule-, and knowledge-based errors or information processing errors including items such as detection and situation assessment)	Does not address unexpected consequences of programed actions
	Loss of communication with software means loss of update capability
	Cannot distinguish between "bad" data and "good"

It's impossible to eliminate all risks, the consequences of eliminating one risk may produce an unexpected result in another area.

III. Reducing Risk; Why Not Just Automate

Humans are always involved, either by direct actions or indirectly during design, development or operational planning. Using software to control systems does not really eliminate the human, since the software codes are written by humans who depend on other humans to provide accurate analysis results and information, catch code errors, perform code downloads, and update software as errors, failures and changes occur.

Also, automated systems do not mean that a human is not involved, someone is always monitoring, modifying and updating. An example is the use of auto-pilot on modern airplanes. A routine airplane flight using autopilot follows a specific flight plan, has defined processes and procedures and performs well as long as all variables stay within the software expectations for system operations. However, abnormal conditions require a human pilot who has the capability and flexibility to make decisions outside the parameters of the auto-pilot programming. For an automated system, identification of requirements, planning, analysis, decision-making and testing is completed prior to use so that the system will react "automatically" to identified data input or set points. Table 3-1 gives a general overview of things to consider when determining how to integrate human capabilities and automation.

Table 3-1: What to Consider When Determining the Use of Human Direction versus Automation

Human More Effective/Efficient	Automated System More Effective/Efficient
When nothing goes as planned or expected	Everything goes as planned or expected
No set routine, needs flexible response	Set routine with limited deviation
Deal with unexpected consequences	Capabilities all identified
Need flexibility in actions for response	Consistent, repetitive actions and activities
Additional capabilities needed beyond original expectations	Immediate response to event needed (too fast for human actions)
Repair small problems to avoid them becoming large problems	Barring software or system failures, always performs as programmed
By adapting to the situation, people often provide the flexibility to "make it work"	Complex or complicated actions needing quick response
Human can be used to mitigate failures	Performs for long durations
When considering outside information and context in decision making ("it depends on…")	When there are no "maybes" in the decision process
Threat detection using multiple subtle cues	Quick response actions for set-points or limits

NOTES:

1. Automated systems can only follow their programming

2. Programming is done by humans based on what they expect to happen
3. Changes to programming (updates) are developed and input by humans

Computerized systems follow the programming. That programming is based on experience and knowledge as well as long hours of analysis, refinement, reviews, simulations, verifications and testing to confirm the expected response occurs. Years of experience with launching vehicles and satellites into space have provided NASA with the knowledge and data to be able to model and predict many aspects of a launch and mission. Spaceflight is a complicated and complex venture, and automated systems (like computers) are tools which used effectively can reduce risk. However, complete reliance on automated systems may not be an effective use since the unexpected generally occurs at some point in the mission.

Manned spaceflight provides for the effective use of a combination of automated actions with human backups when software or other failures occur, or the software cannot address the unfolding event. This is especially true for flight situations which can become problematic for automated systems given the potential for "unknown unknowns" and "underappreciated/underestimated knowns". Regardless of the amount of testing, analysis and experience behind the development of a new vehicle or booster system, progress rarely occurs without unexpected incidents and consequences. The human in the loop, either on the ground or in the vehicle is often the only way to address these unexpected situations. The human in the loop can also provide real time minor corrections that can ultimately avoid multiple small failures resulting in a major failure. These types of efforts are rarely given credit or even recognized as part of the risk avoidance efforts since it's hard to quantify something that didn't or hasn't happened.

On the other side of this issue, there is a plethora of information, documented and speculated, on the subject of human error. In reviewing many of these instances attributed to human error, there are often contributing factors involved that increase the chances of making mistakes. Examples of these types of flaws include:

- Badly designed control panels where switches or buttons are too close together
- Known design problems that use a procedural fix instead of a physical fix
- Procedures that are ambiguous
- Lack of training
- Bad lighting causing visual problems or confusion
- Peripheral items that can contribute to unintended actions

There are methods and techniques to reduce the potential for human error by identifying and addressing these types of issues to eliminate or mitigate conditions that would lead to errors. Using HRA to identify and quantify these risks provides management with additional information for understanding how to address these types of issues.

IV. Identifying What Contributes to Risk and How Much

By understanding what contributes to human action or decision "failures", mitigations can often be recommended, including designs that limit the opportunity for operator errors. Factors that affect crew performance include how these contributing conditions may change during different mission phases. The framework supporting performance of a human action includes the environmental conditions where the action occurs, interfaces with controls or equipment and factors that influence human behavior such as fatigue and training. Human Factors and Operations are involved in human interface issues that affect the crew (such as cabin design, operational processes, procedures and flight rules) and provide support during the mission. Previous NASA experience and lessons learned are implemented in current programs to improve performance. Human reliability assessments at a minimum review the following factors to determine their potential contributions to human error: time to act, complexity and general environment[3]. More in depth methods and techniques such as those addressed in *Cognitive Reliability and Error Analysis Method: CREAM* [4] consider environmental and physical factors which directly impact human performance. These CREAM performance factors include: Adequacy of Organization, Working Conditions, Adequacy MMI (Man Machine Interface) & Operational Support, Availability of Procedures/Plans, Number of Simultaneous Goals, Available Time, Concept of circadian rhythm (used as surrogate for physical, mental and behavioral changes responding to environment), Adequacy training & Preparation and Crew Collaboration Quality.

Efforts to reduce risk associated with crew and ground support personnel actions include:

- NASA trains crew, console controllers and support personnel to solve problems and react to failure scenarios. This includes years of training, simulations, and operational experience.

- NASA uses pre-planning and risk assessment to reduce risks. Models and simulations are used to identify potential problem areas and resolve issues so that these concerns can be eliminated or mitigated prior to launch.
- NASA organizational support and monitoring is continuous, with experts on call. Prior to and during a mission, support staff are available to address any issues that may arise to ensure a safe and successful mission.
- Crew and ground support personnel train for years prior to a mission.

Current program efforts in the design phase provides insights regarding risks contributors for given parameters, allowing a better understanding of overall risk concerns and allow for trade studies as needed. One of the benefits of developing a PRA includes the capability to perform sensitivity analyses. Sensitivity analysis is a useful tool to determine the impact of how changes to the assumptions or variables will differ from the previous or baseline study. By modifying or changing specific variables in the initial scenario, the analyst, operators, and engineers can gain insight into how changes impact the results. Studies can be run on such diverse subjects as determining the importance of a specific component to identifying the impact of changing a basic assumption used as part of the PRA's failure logic model.

V. Human Interactions Can Be Good or Bad

Human error often becomes an error after the fact. The same action can result in a tragic accident for one situation or a heroic action given a more favorable outcome. Human error has been reported as being responsible for 60% - 80%[5] of failures, accidents and incidents in high-risk industries.

E. Hollnagel contends that people in the workplace generally adapt what they do to match the conditions they work in. He describes this as an efficiency-thoroughness trade-off (ETTO)[6]. His concept contends that if the demand for safety is high, resources will be allocated until the safety goals are met, therefore greater "thoroughness" would result in an increase in safety.

NASA Safety and Mission Assurance uses a variety of tools and techniques to ensure that risks are identified and addressed to meet program goals.

The Good

A recent HRA sensitivity study for the new Orion vehicle provided insight into how crew actions associated with mitigation of LOC scenarios would affect the overall risk by comparing the risk associated with the crew's capability to initiate a manual abort and how risk changed with the removal of that capability. The result showed that ~33 % of overall risk was reduced when the crew could perform manual aborts versus having the crew as passengers only. During the Shuttle program, a similar sensitivity assessment was performed which assumed that neither the crew nor the mission control center could take action in response to failures causing a Loss of Crew and/or Vehicle (LOC/V). The difference in the risk when the crew and mission control actively responded to failures showed a risk reduction of ~91%.

The result of the sensitivity studies demonstrate the value of having a highly trained, competent and flexible human backup system for expected and unexpected failures. While HRA assumes that humans will fail a percentage of the time, these studies show what would occur if a crew was not available to make the attempt.

In a human versus computerized system, the human wins in the following areas: flexibility, research, deductions, problem solving, improvisation and troubleshooting. The automated/computerized system wins when: correct actions are known and consistency is paramount, actions need to occur too quickly for humans to react and when humans cannot survive in the environment.

The Bad

The human body also undergoes physical changes such as fatigue, inattention after long hours, medical issues, misunderstanding and miscommunications will always occur. Furthermore, even when the number of goals may be reasonable under most conditions, if multiple operations or short turn-around times due to changing conditions occurs this may impact the crew's reactions. Conditions such as these often occur during critical times of flight such as take-off and landing, or under emergency scenario conditions. These types of situations can overwhelm even the best planning and simulation training. If humans can take direct action to save the vehicle, those actions taken at the wrong time or under the wrong conditions can also result in loss of the vehicle.

VI. Summary

On a really bad day when nothing is going as expected, an automated system gives up (i.e. will only do what it is programmed to do), but a human will keep trying and may succeed. History has shown this to be true during previous NASA missions when problems have occurred. NASA's human spaceflight program crews and support staff are competent, motivated, and experienced individuals who spend years training for each mission. NASA Safety and Mission Assurance spends the time and resources to identify and reduce risk to improve safety.

"To challenge the status quo, organizations must challenge the premise that the human is the weakest link in the workplace. On the contrary, when properly prepared, people are not something to be protected against; they are the strongest part of the performance equation. While technology, technical training and culture are important, the individual mind is more critical."[5]

Spaceflight is a risk, with or without human error.

References

[1]Stamatelatos, Michael et.al, "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners", NASA Office of Safety and Mission Assurance, NASA Headquarters, (2011), Washington. D.C.

[2]Shorrock, Steven, "The Use and Abuse of 'Human Error'", Safety Differently Oct. 18, 2013, http://www.safetydifferently.com/the-use-and-abuse-of-human-error/

[3]Swain, A. D. & H. E. Guttman, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications", NUREG/CR-1278 (1983), Washington D.C.

[4]Hollnagel, E., *Cognitive Reliability and Error Analysis Method: CREAM*, (1998), Elsevier.

[5]Kern, Dr. Tony and David McKay, "The War on Error: Human Error as a Strategic Risk Management Concern", Risk Management May 6, 2013.

[6]Hollnagel, E., *The ETTO Principle: Efficiency-Thoroughness Trade-Off: Why Things That Go Right Sometimes Go Wrong*, (2009), CRC Press.